APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/688,456	10/16/2000	Craig L. Ogg	39778/RRT/S850	1637

23363   7590   03/26/2003

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA   91105

EXAMINER
BACKER, FIRMIN

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 03/26/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/688,456	OGG ET AL.
	Examiner	Art Unit
	Firmin Backer	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *16 October 2000* .

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-70* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-70* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *16 October 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

This is in response to a letter for patent filed on October 16th, 2000 in which claims 1-70 are

presented for examination. Claims 1-70 are pending in the letter.

Double Patenting

1.   The nonstatutory double patenting rejection is based on a judicially created doctrine
grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or
improper timewise extension of the "right to exclude" granted by a patent and to prevent possible
harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed.
Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686
F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA
1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).
        A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to
overcome an actual or provisional rejection based on a nonstatutory double patenting ground
provided the conflicting application or patent is shown to be commonly owned with this
application. See 37 CFR 1.130(b).
        Effective January 1, 1994, a registered attorney or agent of record may sign a terminal
disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37
CFR 3.73(b).

2.   Claims 1-70 are rejected under the judicially created doctrine of obviousness-type double

patenting as being unpatentable over claims 1-71 of U.S. Patent No. 09/690,083. Although the

conflicting claims are not identical, they are not patentably distinct from each other because they

both define inventions that are obvious variations of each other and achieving the same end

result. Accordingly, it would have been obvious to those in possession of the inventive concept

disclosed in claims 1-70 are already included in the inventive concept disclosed in claims 1-71 of

copending application 09/690,083. Furthermore, one of ordinary skill in the art at the time the

invention was made would have realized the inclusion of *"a state machine for determining a*

state corresponding to one or more commands available to an authenticating user" in claim 1,

and the substitution of *"determining a state in a state machine for availability of one or more*

commands" by *"including cryptographically protected data using a stored secret"* in claim 41 of

the copending application 09/690,083 are obvious expedient since the remaining element are

defined in the claims. In re Karlson, 136 USPQ 184 (CCPA 1963).

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1, 7-9, 11-14, 17-36, 39-44, 52-70 are rejected under 35 U.S.C. 102(e) as being

anticipated by Whitehouse (U.S. Patent No. 6,005,945).

5.   As per claim 1, Whitehouse teaches a cryptographic device *(secure central computer,*

102) for securing data *(postal information)* on a computer network *(network 100, fig 3, 4)*

comprising a processor *(postal authority computer for processing, 180)* programmed to

authenticate *(authenticate)* a plurality of users *(users, 104)* on the computer network *(network*

100, fig 3, 4) for secure processing of a value bearing item *(postal indicium, fig 2) (see*

abstract, figs 2, 3, 4), a memory *(memory, 154)* for storing *(stores)* security device transaction

data *(records)* for ensuring authenticity of a user, wherein the security device transaction data

is related to the one of the plurality of users a cryptographic engine *(cryptographic key)* for

cryptographically protecting data and an interface *(interface, 152, 112, 252)* for

communicating with the computer network *(see abstract, fig 4, 7, column 8 lines 54-8 line 63)*.

6.   As per claim 7-9, Whitehouse teaches a cryptographic device further comprising a

stored secret that is a password, a public/private key for cryptographically protecting data *(see*

column 8 lines 30-42, 9 lines 12-31, 10 lines 50-11 line 29, 12 lines 35-64).

7.   As per claim 11-14, Whitehouse teaches a cryptographic device wherein the processor is

stateless and is programmed to for preventing unauthorized disclosure of data and undetected

modification of data, to ensure proper operation of cryptographic security and VBI related meter

functions *(see abstract, figs 3, 4, 6 and 7, column 12 lines 35-64, 13 line 61-14 line 36)*.

8.   As per claim 17, Whitehouse teaches a cryptographic device wherein the processor

stores information about a number of last transactions in an internal register and compares

the information saved in the register with the information saved in a memory before loading

a new transaction data *(see column 13 lines 61-65, 14 lines 25-36, 21 lines 20-45)*.

9.   As per claim 18, Whitehouse teaches a cryptographic device wherein the memory

includes data for creating indicium, account maintenance, and revenue protection (*see figs 4,*

and 7).

10.   As per claim 19-22, Whitehouse teaches a cryptographic device wherein the value

bearing item is a postage value including a postal indicium comprises a digital signature and

a postage amount, an ascending register of used postage and descending register of available

postage (*see abstract, column 16 lines 25-38).*

11.   As per claim 23-28, Whitehouse teaches a cryptographic device wherein the value

bearing item that include a bar code is a ticket, a coupon, currency, a voucher, a traveler's

check (*fig 2).*

12.   As per claim 29, Whitehouse teaches a cryptographic device wherein each security

device transaction data includes an ascending register value, a descending register value, a

respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP

code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets,

data and time of last transaction, last challenge received from a respective client subsystem, an

operational state of the respective device, expiration dates for keys, and a passphrase repetition

list (*see column 10 line 45-11 line 29, 20 line 16-40).*

13.　　As per claim 30, Whitehouse teaches a cryptographic device wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices (*see column 9 line 32-50*).

14.　　As per claim 31-34, Whitehouse teaches a cryptographic device wherein the processor and the cryptographic engine generate a master key set (MKS) includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device, includes a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device and is exported to other cryptographic devices (*see column 23 line 41-67*).

15.　　As per claim 35, Whitehouse teaches a cryptographic device comprising a memory including a user profile for a subset of the plurality of users (*see column 10 line 45-11 line 29*).

16.　　As per claim 36, Whitehouse teaches a cryptographic device wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period (*see column 10 line 45-11 line 29*).

17.　　As per claim 39, Whitehouse teaches a cryptographic device wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (*see column 4 line 20-27, 16 lines 39-44, 23 lines 41-67*).

18.   As per claim 40, Whitehouse teaches a cryptographic device wherein at least one of the

plurality of users is an enterprise account *(see column 27 lines 27-45)*.

19.   As per claim 41, Whitehouse teaches a method for securing *(secure central computer,*

102) data *(postal information)* on a computer network *(network 100, fig 3, 4)* including a

plurality of users *(customer/users, 104)* comprising authenticating *(authenticate)* and

authorizing *(authorizing)* the plurality of users *(customer/users, 104)* for secure processing of a

value bearing item *(postal indicium, fig 2) (see abstract, figs 2, 3, 4)*, storing *(storing)* a

security device transaction data *(cryptographic key record)* in a memory *(memory, 154)* for

ensuring authenticity and authority of one of the plurality of users, wherein the security device

transaction data is related to the one of the plurality of users and including cryptographicaily

protected data using a stored secret *(key) (see abstract, fig 4, 7, column 8 lines 54-8 line 63)*.

20.   As per claim 42, Whitehouse teaches a method of printing the value bearing item *(see*

figs 2, 5).

21.   As per claim 43, Whitehouse teaches a method of storing a plurality of security device

transaction data related to one of the plurality of users *(see column 9 lines 12-31)*.

22.   As per claim 44, Whitehouse teaches a method of loading a security device transaction

data related to the cryptographic device when the user requests to operate on a value bearing

item *(see column 9 lines 12-31)*.

23.   As per claim 52-55, Whitehouse teaches a method further comprising the step of

printing a postage value including a postal indicium comprises a digital signature, a postage

amount, an ascending register of used postage and descending register of available postage

(see column 16 lines 25-38).

24.   As per claim 56-61, Whitehouse teaches a method of printing a ticket, a bar code, a

coupon, a currency, a traveler's check, a voucher *(see fig 2)*

25.   As per claim 62, 63, Whitehouse teaches a method of storing a user profile includes

username, user role, password, logon failure count, Logon failure limit, logon time-out limit,

account expiration, password expiration, and password period for a subset of the plurality of

users *(see column 10 line 45-11 line 29)*.

26.   As per claim 64, Whitehouse teaches a method of performing one or more of Rivest,

Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1,

and Pseudo-random number generation algorithms by each of the cryptographic devices *(see*

column 4 line 20-27, 16 lines 39-44, 23 lines 41-67).

27.   As per claim 65, Whitehouse teaches a method of supporting multiple concurrent

operators and maintaining a separation of roles and operations performed by each operator (*see*

fig 3).

28.   As per claim 66, Whitehouse teaches a method of storing information about a number of

last transactions in a respective internal register of each of the one or more cryptographic

devices, storing a table including the information about a last transaction in the database; and

comparing the information saved in the respective device with the respective information saved

in the database (*see column 10 line 45-11 line 29*).

29.   As per claim 67, Whitehouse teaches a method of loading a new transaction data if the

respective information stored in the device compares with the respective information stored in

the database (*see column 22 line 36-53*).

30.   As per claim 68-69, Whitehouse teaches a method therein the secret is a password, a

public/private key pair (*see column 8 lines 30-42, 9 lines 12-31, 10 lines 50-11 line 29, 12 lines*

35-64).

31.   As per claim 70, Whitehouse teaches a method wherein at least one of the plurality of

users is an enterprise account (*see column 27 lines 27-45*).

Claim Rejections - 35 USC § 103

32. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

33. Claims 2-6, 10, 15, 16, 37, 38 and 45-51, rejected under 35 U.S.C. 103(a) as being

unpatentable over Whitehouse (U.S. Patent No. 6,005,945) in view of Leon (U.S. Patent No.

6,424,954).

34. As per claims 2 and 45 Whitehouse teaches the inventive concept as stated in claim 1.

Whitehouse fail to teach a cryptographic device and a method wherein the processor is

programmed to verify that the identified user is authorized to assume a role and perform a

corresponding operation. However, Leon teaches a cryptographic device wherein the processor

is programmed to verify that the identified user is authorized to assume a role and perform a

corresponding operation (*see column 8 line 45-9 line 67*). Therefore, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to modify

Whitehouse's inventive concept to include Leon a cryptographic device wherein the processor

is programmed to verify that the identified user is authorized to assume a role and perform a

corresponding operation because this would have provided knowledge to the system as to which

entity is using the system in order to determine which level of security is applicable.

35.   As per claim 3-6, 46-51, Leon teaches a cryptographic device wherein the assumed role

is a key custodian role to take possession of shares of keys, an administrator role to manages a

user access control database, is a provider role to authorize increasing credit for a user account

a user role to perform expected IBIP postal meter operations (*see column 8 line 45-9 line 67*).

36.   As per claim 10, Leon teaches a cryptographic device wherein the processor is

programmed to include a state machine for determining a state corresponding to availability of

commands in conjunction with the roles (*see column 8 lines 45-62*).

37.   As per claims 15 and 16, Leon teaches a cryptographic device for providing indications

of an operational state of a VBI meter, for supporting multiple concurrent users and maintaining

a separation of roles and operations performed by each user (*see column 8 lines 45-62*).

38.   As per claim 37, Whitehouse teaches a cryptographic device wherein the state machine

comprises of an uninitialized state, an initialized state, an operational state, an administrative

state, an exporting shares state, an importing shares state, and an error state (*see fig 6A, column

9 line 59-62*).

39.   As per claim 38, Whitehouse teaches a cryptographic device wherein the operational

state comprises means for access control, session management, key management, audit support

(*see column 10 line 1-11 line 34*).

40. As per claim 45, Whitehouse teaches a method authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation (*see abstract*).

Conclusion

41. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

    a. *Cordey et al (U.S. Patent No. 6,466,921) teach a virtual postage metering system provides central management of all postage without the need to manage physical meters or PSDs.*

    b. *Amanda (U.S. Patent No 6,385,731)) teaches on-line electronic postage metering system that operates in conjunction with the United States Postal Service (USPS) that allows a user to print a postal indicium at home, at office, or any other desired place in a secure and fraud-free manner. A user computer and a user printer, electronically connected to the PSD server and the USPS computer, constitute an on-line electronic postage meter.*

    c. *Kara et al (U.S. Patent No. 6,249,777) teach a demand program that may be coupled to a word processing program, or other process, residing within the first PC,*
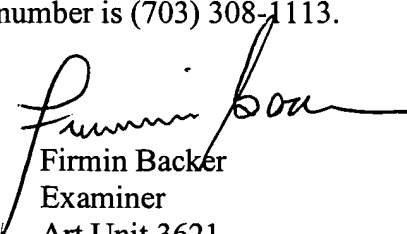
thus allowing the user to request and subsequently print the postage indicia on

correspondence or postal items generated by the coupled process.

d.   *Leon (U.S. Patent No. 6,381,589) teaches a secure processing unit interfaces with*

the local computer and performs the secure processing normally associated with a secure

postal environment.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The

examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, James Trammell can be reached on (703) 305-9768. The fax phone numbers for the

organization where this application or proceeding is assigned are (703) 305-7687 for regular

communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is (703) 308-1113.

Firmin Backer
Examiner
Art Unit 3621

March 13, 2003